v. After decryption, the server reports to an inquiring party,

1. whether an electronic data submitted for verification remains unmodified since a signature was affixed, and
2. the identity of a signer of the electronic data.

77. The method of claim 76 wherein the electronic data set which is symmetrically encrypted during signature and decrypted upon verification at a server consists of one of the following:

a. A message digest or hash of the electronic data;
b. A crypto-transformation, created using a private key, of the message digest or hash of the electronic data.

78. The method of claim 76 wherein the electronic data submitted for signature consists of one of the following:

a. Form input of a signer;
b. A combination of form input of a signer and standardized words, clauses, or phrases.

REMARKS – General

In a telephone conversation dated June 10, 2002, the Applicant and Examiner discussed a web demonstration of the invention. Applicant's summary is enclosed.

Applicant believes that the summary will be helpful in answering the question raised in the Office Action dated June 20, 2002 on page 3, which asked as follows: "The examiner is not sure though, what benefit is accrued from the private key signing. Haven't the benefits from the public key signing should already been realized through the symmetric key signing?"

The Applicant apologizes for the confusion and has proposed adding a clause to the specification as set out above. Applicant has attempted to clarify how the symmetric encryption

works together ***with*** the preferred asymmetric embodiment of the invention, and not simply as an alternative to it. The asymmetrically encrypted RSA signature value returned by the web program is in turn itself encrypted by a second symmetric cipher. The symmetric cipher is indirectly derived from the identity of the signer in the formulation of the GUID. In order to be able to decrypt the asymmetric signature value and verify the signature, the symmetric encryption involving the signer's identity must be decrypted first; otherwise, asymmetric signature verification using a public key is impossible. In this way, the identity of the signer becomes cryptographically wrapped around the asymmetric signature of the server's key; hence the terminology in the specification of a "digital wrapper." The Applicant attempted to point out that this combination in the telephone conversation with the Examiner in order to point out that it had the further advantage of protecting the private key of the server from a potential vulnerability otherwise occasioned from its constant use for signature transactions. Without the symmetric digital wrapper that changed with each signer transaction, an attacker might be able to deduce the private key attributes from an examination of a myriad of signatures and hash values. The symmetrically encrypted signature value also can serve to protect the underlying asymmetric signature at a future time when a factoring attack on asymmetric RSA signatures by significantly more powerful computers may become computationally feasible. The symmetric encryption of the returned asymmetric signature value may act as an added shield to protect the asymmetric private key from a factoring attack as the symmetric enciphering wrapper cloaks the asymmetric signature value, hiding it from the attacker. The Applicant opined to the Examiner this embodiment of the invention was novel as against prior art.

The Office Action objected to claim 63 as dependent upon a rejected claim 56. Applicant has cancelled certain dependent claims and rewritten claim 63 in combination with claim 56 as new claim 76 in accordance with paragraph 12 of the Office Action entitled: "Allowable Subject Matter", and has added two dependent claims.

Conclusion

For all of the above reasons, applicant submits that the specification and claims are now in proper form, and that the amended claims all define patentability over the prior art. Therefore, applicant submits that this application is now in condition for allowance, which action is respectfully solicited.

Very respectfully,

John H. Messing
Applicant Pro Se

6571 N. Silver Smith Place, Tucson, AZ 85750
Tel.: (520) 547-7933 or (520) 529-3275 Fax: (520) 529-3204

Certificate of mailing: I certify that on the date below this document and referenced documents and attachments will be deposited with the U.S. Postal Service as first class mail in an envelope addressed to: "BOX AF, ASSISTANT COMMISSIONER FOR PATENTS, WASHINGTON, D.C. 20231."

August 13, 2002

John H. Messing
Applicant